

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

L'affaire Napster ou le difficile équilibre entre le droit d'auteur et le respect de la vie privée

De Patoul, Fabrice; Rue, Guillaume

Published in:
Revue Ubiquité. Droit des technologies de l'information

Publication date:
2002

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):
De Patoul, F & Rue, G 2002, 'L'affaire Napster ou le difficile équilibre entre le droit d'auteur et le respect de la vie privée', *Revue Ubiquité. Droit des technologies de l'information*, Numéro 12, p. 7-29.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

L'affaire Napster ou le difficile équilibre entre le droit d'auteur et le respect de la vie privée

**Guillaume Rue^{1 2}
Fabrice de Patoul³**

1. INTRODUCTION

La Revue Ubiquité s'est faite, à de multiples reprises, l'écho des défis auxquels se trouve confronté le droit face aux développements des nouvelles technologies. Le droit d'auteur est particulièrement sollicité dans une économie de réseau où l'information numérisée devient une nouvelle matière première. Les créateurs, diffuseurs ou éditeurs de ces informations s'interrogent légitimement sur la protection de leurs droits dans le monde numérique.

Dans ce contexte, l'affaire Napster a agi comme un révélateur de l'ampleur des infractions au droit d'auteur réalisables par Internet. Des milliers de morceaux de musique en format compressé se sont ainsi échangés à la vitesse de l'éclair entre les disques durs des internautes du monde entier. Ces atteintes au droit d'auteur n'ont pas manqué de faire réagir l'industrie du disque. Ainsi, en Belgique, la branche belge de l'IFPI⁴ a procédé à des recherches sur les utilisateurs belges du site de Napster qui mettaient à disposition ou téléchargeaient des morceaux d'artistes belges. Cette recherche s'est opérée selon un modus operandi assez étonnant. D'abord, le représentant de l'IFPI s'est enregistré sur le site sous un pseudonyme comme tout utilisateur classique désirant se servir de Napster. Ensuite, il a effectué une recherche des morceaux d'artistes belges disponibles via Napster et a débuté un téléchargement. C'est au cours de celui-ci que l'IFPI va pouvoir, grâce à une fonction logicielle, déterminer l'adresse IP⁵ de l'internaute qui met à disposition illégalement les morceaux de musique. Enfin, cette adresse IP va être communiquée par l'IFPI au fournisseur d'accès concerné afin que ce dernier identifie l'internaute contrefacteur. Dans un premier temps, celui-ci recevra de son fournisseur d'accès une mise en demeure de cesser tout comportement délictueux et, en outre, devra effacer tout morceau illégalement téléchargé. En cas de récidive de l'intéressé, l'IFPI dénonce alors les faits au parquet.

Bien que l'objectif des recherches, menées par l'IFPI, puisse apparaître comme légitime, il y a lieu de s'interroger sur la méthode employée par cette association privée pour arriver à ses fins. En effet, les moyens mis en œuvre méritent d'être examinés au regard des dispositions juridiques protégeant les données à caractère personnel et les télécommunications. Un avis de la commission de la protection de la vie privée, publié dans cette revue, est particulièrement éclairant à cet égard et nous ne manquerons pas d'y référer.⁶ On le comprend, deux logiques appartenant à deux domaines du droit viennent ici s'entrechoquer. D'un côté, le droit d'auteur qui entend protéger les créateurs et leur assurer une juste rémunération de leur travail. De l'autre, le respect de la vie privée ou du secret des télécommunications qui fixe comme priorité le respect des libertés individuelles. Il y aura lieu de voir comment une cohérence peut être apportée au cadre juridique existant face aux nouvelles pratiques engendrées par Internet. Tel sera l'objet de cet article.

¹ Les auteurs tiennent à remercier Séverine Dusollier pour ses précieux conseils dans la rédaction de cet article.

² Avocat au Barreau de Bruxelles - diplômé du DGTIC 2000-2001.

³ Chercheur au Crid - diplômé du DGTIC 2000-2001.

⁴ IFPI-Belgium : International Federation of the Phonographic Industry ou la Fédération Internationale de l'Industrie Phonographique.

⁵ IP pour Internet Protocol (cf. *infra*)

⁶ La Commission de la protection de la vie privée a rendu un avis d'initiative concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant le caractère personnel et les télécommunications. Avis N°44/2001 du 12 novembre 2001.

Une première partie fera un rapide tour d'horizon des questions de droit d'auteur qui se posent vis-à-vis des logiciels d'échange de fichiers. La seconde partie abordera la matière sous l'angle de la protection des données à caractère personnel et des télécommunications. Par ailleurs, nous profiterons de cette introduction pour rappeler les différentes avancées technologiques qui sont à l'origine de la situation actuelle.

1.1. L'INFORMATION EN FORME NUMERIQUE FACILITE LA REPRODUCTION

En matière de droit d'auteur, la digitalisation de l'information a deux conséquences importantes.⁷

D'une part, les barrières naturelles à la reproduction du monde analogique s'estompent. Auparavant, la reproduction était naturellement limitée par la perte en qualité dans les copies analogiques successives et par le coût qu'impliquait une reproduction de qualité. La numérisation des données permet aujourd'hui de réaliser des copies parfaites de l'original et de manière moins coûteuse. A son tour, chaque copie devient un nouvel original (*master copy*) qui peut être dupliqué. La maîtrise de l'œuvre par son auteur ne dépend plus des copies qu'il délivre. En effet, une seule copie de l'œuvre peut être disséminée de manière infinie et est susceptible d'innombrables utilisations simultanées par de multiples utilisateurs. L'auteur recherche, dès lors, de nouveaux moyens de retrouver la mainmise sur son œuvre par la mise en place de systèmes techniques de protection ou de systèmes de gestion de droit d'accès.

D'autre part, l'accès et l'utilisation de l'information digitale impliquent obligatoirement la réalisation de nombreuses copies éphémères. Ainsi, l'accès à des données informatiques stockées sur l'ordinateur nécessite une copie temporaire sur la mémoire vive de l'ordinateur (RAM).⁸ Cette copie fugitive disparaît néanmoins dès que l'on éteint l'ordinateur. L'utilisation de réseaux, tel qu'Internet, rend également nécessaire la création d'une multitude de copies provisoires non seulement sur l'ordinateur du destinataire mais également sur l'ensemble des serveurs, routeurs et autres systèmes de transmission utilisés par les intermédiaires techniques.

1.2. LES RESEAUX INFORMATIQUES FACILITENT LA DISTRIBUTION ET LA DIFFUSION

Le développement des réseaux permet le transfert rapide des données binaires. En outre, grâce à différents modes de compression des données, on parvient à améliorer la capacité des réseaux qui sont en mesure de transporter de plus grandes masses d'informations. Ainsi, des œuvres audiovisuelles, des images ou des logiciels peuvent être transférés à haut débit grâce à un ensemble de réseaux de télécommunication.

L'utilisation d'Internet facilite, dès lors, la diffusion et la publication, sous forme «numérique», d'œuvres protégées par le droit d'auteur. La technologie rend la distribution plus facile, plus rapide et moins coûteuse.

⁷ Dans la société de l'information, on a tendance à penser que le droit d'auteur protège l'information alors que celui-ci est d'abord conçu en vue d'assurer la protection des œuvres, c'est-à-dire les formes originales et personnelles d'expression. Cet amalgame, ou ce malentendu, provient sans doute notamment du fait que la numérisation réalise un nivellement entre l'information et les œuvres en données binaires. Voy. A. STROWEL, « Droit d'auteur et accès à l'information : de quelques malentendus et vrais problèmes à travers l'histoire et les développements récents », *Les Cahiers de la propriété intellectuelle*, 2000, p. 185 et s.

⁸ P. SAMUELSON & R. DAVIS, *The Digital Dilemma : A Perspective on Intellectual Property in the Information Age*, Computer Science & Telecommunication board, Intellectual Property in the Information Age, 2000, p. 9.

a. Caractéristiques du réseau

Deux caractéristiques propres aux réseaux ont été relevées par S. DUSOLIER : la disparition des supports, d'une part, et, celle des intermédiaires, d'autre part.⁹

La disparition du support ou la *dématérialisation* constitue une nouveauté fondamentale par rapport à l'univers analogique. Au lieu d'acheter un disque, on peut accéder de manière limitée à la musique contenue sur ce disque via les réseaux. En d'autres termes, l'acquisition d'un support est remplacée par le paiement d'un droit d'accès, sous forme d'abonnement, à la musique qui reste stockée sur la base de données de l'auteur. Cependant, une certaine évolution des mentalités est nécessaire pour arriver au monde de la « musique dématérialisée ». Dans un premier temps, des solutions de téléchargement sécurisé seront sans doute privilégiées de manière à ce que l'utilisateur possède encore une copie numérique non-dupliquable de l'œuvre musicale sur son ordinateur.

La disparition des intermédiaires ou la *désintermédiation* constitue la seconde transformation fondamentale sur les canaux de distribution réalisée par les réseaux numériques. Les intermédiaires classiques qui assuraient la commercialisation et l'exploitation des œuvres peuvent être contournés dans l'environnement digital. Un rapport direct entre l'utilisateur et l'auteur s'instaure, où ce dernier entend garantir une protection de l'accès à son œuvre.

b. Les conséquences du contexte des réseaux numériques

Le contexte digital apporte un premier changement radical sur l'utilisation des œuvres et des contenus culturels. Auparavant, on achetait un support au distributeur, ainsi rétribué de son service, tandis que désormais, on paie directement l'auteur pour l'accès ou l'utilisation de son œuvre. Une transition s'opère doucement vers un modèle économique où ne sera facturé à l'utilisateur final non plus le prix de l'acquisition du support mais bien la consultation, la mise à disposition ou le temps de connexion au contenu numérique culturel ou scientifique.¹⁰ Par des contrats et des mesures techniques, l'auteur retrouve la mainmise sur son œuvre. En effet, il contrôle l'accès à son œuvre et, dès lors, l'usage qui en est fait.

Une deuxième conséquence directe de l'environnement de réseaux numériques est le rôle grandissant joué par les particuliers. Ce dernier aspect n'est pas souvent mis en évidence dans le débat qui entoure les droits de la propriété intellectuelle. Auparavant, les atteintes les plus dommageables au droit d'auteur étaient principalement le fait d'un petit nombre de personnes organisées avec des moyens importants. Dans le monde des réseaux, l'atteinte au droit d'auteur se caractérise par la multiplication d'atteintes commises par des particuliers sans investissement important. Un ordinateur personnel et une connexion au réseau sont suffisants pour obtenir une photo, une chanson ou copier un article et l'envoyer à un ami par e-mail. La prolifération d'infractions à petite échelle, due entre autres à la forte simplification de l'utilisation des technologies, se combine avec une relative méconnaissance du grand public de la portée de ses actes. En effet, la ligne tracée entre l'illégalité et la légalité apparaît comme floue pour le citoyen habitué à la copie analogique sur cassette audio et vidéo. Or, aujourd'hui, le succès d'un logiciel comme Napster, et de la technologie *peer to peer*, que ce programme applique, témoigne de l'importance croissante que prennent les particuliers dans le monde des réseaux.¹¹

⁹ S. DUSOLIER, « Incidences et réalités d'un droit de contrôler l'accès en droit européen », in *Le Droit d'auteur : un contrôle de l'accès aux œuvres ?*, Cahier du CRID n°18, Bruylant, 2000, p. 27 et s.

¹⁰ S. DUSOLIER, *ibidem*, p. 27.

¹¹ P. SAMUELSON & R. DAVIS, *The Digital Dilemma : A Perspective on Intellectual Property in the Information Age*, Computer Science & Telecommunication board, Intellectual Property in the Information Age, 2000, p. 9.

1.2. LES ELEMENTS TECHNIQUES

Pour donner toutes les clés de compréhension au lecteur, il nous a semblé utile d'expliquer brièvement les éléments techniques dont il est question dans l'affaire Napster.

a. La norme MPEG-1 Audio Layer 3 Compression (MP3)

La facilité et la rapidité d'échange de fichiers sur les réseaux sont tributaires de la capacité des lignes mais aussi de la taille des fichiers à diffuser. Ainsi, pour accélérer la transmission des fichiers, une des solutions envisagées consiste à compresser la taille de ceux-ci. La norme MP3 est un standard de compression de données qui permet de compresser de 10 à 12 fois les fichiers audio traditionnels sans aucune perte de qualité.¹² Outre cet avantage technique, le format MP3 présente l'avantage d'avoir été reconnu internationalement¹³ et fait ainsi partie des normes MPEG (Moving Picture Experts) qui sont un ensemble de standards internationaux utilisés pour la codification des informations audiovisuelles dans un format digital compressé. Pour comprendre la puissance de cette technologie, il faut savoir qu'un CD peut contenir 150 chansons au format MP3 soit l'équivalent de 12 disques compacts. La facilité d'utilisation et surtout la taille réduite du format MP3 l'a naturellement conduit à être utilisé sur Internet.

b. La technologie Peer -to-peer (P2P)

Auparavant la structure du *World Wide Web* pouvait être schématiquement décrite comme une pyramide hiérarchisée avec, à son sommet, des *serveurs* contenant un grand nombre de pages webs et, à sa base, des *clients* qui, depuis leurs ordinateurs, chez eux ou au bureau, se connectent à ceux-ci. Le contenu d'Internet se trouvait dès lors, principalement, sur ces serveurs appartenant pour la plupart à des entreprises spécialisées. Les particuliers, qui créent un site web, profitent généralement des possibilités d'hébergement (*hosting*) qui leur sont offertes sur ces serveurs.

La révolution opérée par la technologie P2P consiste à renverser ce traditionnel schéma client-serveur. En effet, dans ce modèle, chaque ordinateur individuel devient à son tour un serveur et apporte son contenu au réseau et inversement. En d'autres termes, tout client est potentiellement serveur pour un autre client. Si chaque ordinateur peut parler à ses pairs, les ressources du réseau auparavant inexploitées peuvent être mises en commun et utilisées par d'autres.

c.- Présentation et fonctionnement du logiciel Napster

Napster est un logiciel qui permet l'échange de fichiers entre les disques durs des utilisateurs sans aucun paiement. Comment cela se déroule-t-il concrètement ? Les utilisateurs téléchargent gratuitement ce logiciel depuis le site de Napster.com et peuvent ensuite accéder, grâce à leur ordinateur, à un des 150 serveurs avec lequel le système Napster opère. Lors de sa connexion, le logiciel *MusicShare* recense la liste des titres que l'utilisateur veut rendre disponibles et les ajoute à la liste de titres des autres personnes déjà connectées sur le serveur. Ensuite, l'utilisateur sélectionne une chanson sur un des serveurs et le système Napster met

¹² Il n'y a aucune perte de qualité car la compression est rendue possible par la suppression des données inaudibles pour l'oreille humaine (ultrasons et infrasons) ainsi que la suppression des sons d'instruments inaudibles parce que joués en même temps que d'autres instruments qui les masquent.

¹³ J. FOLON et R. BAILLY, « La musique on line : une nouvelle gestion du droit d'auteur et des droits voisins ? », *Revue Ubiquité*, mai 1999, n°2, F.U.N.D.P., p. 84.

directement en communication les deux internautes. Il est important de noter que les chansons ne sont pas «physiquement» stockées sur le serveur lui-même mais restent sur les disques durs des utilisateurs. Napster permet seulement de recenser les titres et facilite les téléchargements entre deux utilisateurs.

2. LES QUESTIONS DE DROIT D'AUTEUR FACE AUX LOGICIELS D'ECHANGE

2.1. LE CADRE LEGAL BELGE

La loi du 30 juin 1994¹⁴ régit la matière du droit d'auteur et des droits voisins depuis l'abrogation de la loi du 22 mars 1886. Cette loi rédigée en des termes relativement larges et neutres a réussi à encadrer, dans la mesure de ses moyens, les différentes évolutions technologiques auxquelles elle a dû faire face en un peu moins de dix ans d'existence. Elle doit cependant affronter des problèmes spécifiques et inédits liés à l'émergence des nouvelles technologies et à l'internationalisation de l'exploitation des oeuvres. Cette nouvelle situation fut une des raisons de la signature des deux traités au sein de l'OMPI¹⁵, et que l'Union européenne a traduit en droit européen par la directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.¹⁶ Un avant-projet de loi belge visant à transcrire cette directive dans la législation belge est en cours d'élaboration.¹⁷

Par souci de concision de l'exposé, nous ne rappellerons pas quelles sont les conditions de protection de ces œuvres, ni dans quelle mesure un fichier MP3 peut en bénéficier. La reproduction d'une chanson en format de compression MP3 tombe sans aucun doute sous l'application de la loi. Il s'agit de la reproduction d'une création musicale, déjà elle-même en principe originale, sous une forme numérisée qui constitue une écriture ou une expression de l'œuvre. Le droit d'auteur protège toute composition musicale pourvu qu'elle soit originale, condition supposée remplie par l'œuvre musicale avant compression, et pourvu aussi qu'elle existe dans une forme particulière, ici le MP3.

En ce qui concerne la titularité des droits¹⁸, un fichier MP3 indique généralement le nom de l'interprète et le nom de sa composition. Cependant, il est facile pour n'importe quel utilisateur de remplacer le nom du fichier grâce à une simple manipulation. Outre la question du droit moral de paternité qui pourrait se poser, il sera difficile d'accorder une quelconque présomption de titularité en faveur de la personne qui a indiqué son nom de cette manière. La technologie peut jouer un rôle important dans ce domaine en assurant le marquage des œuvres de façon indélébile au moyen d'outils cryptographiques *ad hoc*. Ainsi, il est possible d'établir un lien certain entre la musique et certaines informations afin de permettre une traçabilité des œuvres musicales (auteur, interprète, date de mise en circulation, etc.).¹⁹

¹⁴ Loi du 30 juin 1994 relative aux *droits d'auteur et aux droits voisins*, M.B. 27 juillet 1994, p. 19297-19134. Modifié par la loi du 31 août 1998, M.B., 14 Novembre 1998, p. 36914.

¹⁵ Il s'agit du Traité de l'OMPI sur le droit d'auteur et du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes, signés à Genève le 20 décembre 1996.

¹⁶ Directive (C.E.) 2001/29 du 22 mai 2001 du Parlement européen et du Conseil sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (*J.O. L* 167, 22 juin 2001, p.10).

¹⁷ Voy. le site du Ministère de la Justice <http://www.just.fgov.be/>

¹⁸ article 6, alinéa 1^{er} et 2nd, de la LDA

¹⁹ S. DUSOLLIER, « Le droit d'auteur et son empreinte digitale », *Ubiquité*, n°2, Mai 1999, p.31-47 ; J. FOLON, R. BAILLY, *op. cit.*, mai 1999, n°2, F.U.N.D.P., p. 74.

2.2. LES PREROGATIVES DE L'AUTEUR

On distingue habituellement les prérogatives patrimoniales et les prérogatives d'ordre moral de l'auteur. Ainsi, l'auteur est titulaire de droits « économiques », c'est-à-dire des droits relatifs à l'exploitation de l'œuvre, et des droits moraux qui visent à protéger des intérêts liés à la personnalité de l'auteur.²⁰ Seuls les premiers seront évoqués ici.

a.- Le droit de reproduction (art. 1^{er} §1 alinéa 1)

La délimitation large du droit de reproduction permet de nouvelles applications dans la société de l'information. En effet, un grand nombre d'actions sont facilitées par l'utilisation des nouvelles technologies. La numérisation des données et l'usage d'Internet permettent de nouvelles formes d'utilisations telles que le *browsing* (navigation), le *downloading* (pu téléchargement) et le *uploading* (ou mise à disposition)²¹ Il a fallu se poser la question de savoir dans quelle mesure le champ de la notion de droit de reproduction pouvait englober ces nouveaux modes d'exploitation des œuvres.

La numérisation et la mise à disposition sur le réseau Internet d'une œuvre protégée par le droit d'auteur ont été considérées par la jurisprudence²² et la doctrine²³ comme soumis à l'autorisation de l'auteur. Ainsi, le simple stockage d'un fichier MP3 sur la mémoire d'un ordinateur ou sur une disquette est une reproduction soumise au contrôle de l'auteur. De plus, cette approche large de la notion de droit de reproduction permet d'y inclure également la mise à disposition sur le réseau (« uploading ») ou le téléchargement (« downloading ») qui sont donc également soumis à l'autorisation de l'auteur. Par ailleurs, l'exception de l'article 5 de la directive en matière de droit d'auteur, qui exempte à certaines conditions la reproduction temporaire, ne peut être invoquée dans cette hypothèse. Un téléchargement, par exemple, n'est pas provisoire, ni transitoire ou accessoire car il demeure sur le disque dur de l'utilisateur.

Il nous apparaît que l'internaute qui utilise le logiciel Napster porte atteinte au droit exclusif de reproduction de l'auteur en stockant, mettant à disposition ou en téléchargeant des œuvres musicales protégées. Ce sont des actes de reproduction qui sont soumis à l'autorisation de l'auteur, de l'artiste interprète et des producteurs de phonogramme.

Une autre question est celle de savoir si la société titulaire du logiciel Napster porte atteinte au droit d'auteur. Une jurisprudence américaine considère que Napster était co-responsable (*contributory liable*) dans la mesure où il avait une connaissance réelle qu'un contenu protégé par le droit d'auteur était disponible grâce à son système et ne prenait pas les mesures adéquates pour l'enlever. En outre, selon le juge américain, le système Napster permet majoritairement des utilisations illégitimes.²⁴

b. – Le droit de communication au public (art. 1^{er} §1 alinéa 4)

²⁰ A. STROWEL et J.-P. TRIAILLE, *op. cit.*, p. 29, n°35.

²¹ Dans le cadre de cet exposé, nous nous limiterons aux applications possibles résultant de la numérisation des œuvres musicales. Nous n'aborderons pas d'autres questions telles que le droit de reproduction des textes de chansons ou le droit de reproduction pour les partitions. Voyez J. FOLON et R. BAILLY, « La musique *on line* : une nouvelle gestion du droit d'auteur et des droits voisins ? », *Revue Ubiquité*, mai 1999, n°2, F.U.N.D.P., p. 68 et s.

²² Voy. not. Trib. 1^{ère} Inst., Bruxelles, 16 octobre 1996, *R.I.D.A.*, avril 1997, n°172, p. 238 ; Bruxelles, 28 Octobre 1997, *R.I.D.A.*, juillet 1998, n°177, p.204.

²³ A. LUCAS, *Droit d'auteur et Numérique*, Litec, Paris, 1998, p. 120, n°241-242 ; A. STROWEL et J.-P. TRIAILLE, *op. cit.*, p. 393, n°517.

²⁴ Napster ne pouvait être tenu comme directement responsable car elle ne stockait, ne copiait pas ni ne distribuait elle-même la musique protégée. *A&M Records, Inc. v. Napster, Inc.*, Court of Appeal (9th circuit), n°00-16401, 28 juillet 2000.

Les œuvres musicales sont soumises à l'autorisation de leur auteur, non seulement en vertu du droit de reproduction mais aussi pour leur diffusion sur les réseaux. Cette diffusion constitue-t-elle une communication au public ?

La notion centrale de ce droit est le caractère public ou non de la communication. Pour déterminer l'étendue du concept de « public », on recourt généralement à un raisonnement *a contrario* en partant de la notion de communication privée énoncée à l'article 22, §1, 3° comme « *la communication gratuite et privée effectuée dans le cercle de famille* ». Cette définition restrictive laisse penser que la notion de « public » doit être entendue de manière large, d'autant plus, qu'un amendement visant à étendre la notion de communication privée avait été rejeté.²⁵

Lorsque deux internautes s'échangent des fichiers MP3 via les réseaux sans passer par un serveur central, peut-on parler réellement d'une communication à un « public » ? Le simple fait de posséder des fichiers MP3 sur son disque dur lorsqu'on se connecte à un logiciel d'échange de fichiers, tel Napster, constitue-t-il une mise à la disposition du public ? La mise à disposition de fichiers MP3 sur un site Internet, ou même par l'intermédiaire de liens y renvoyant, peut constituer une communication au public. Il nous semble raisonnable de soutenir que l'internaute, qui utilise Napster, réalise une communication au public des fichiers qu'il possède, même si le transfert se réalise entre deux personnes.

La spécificité des nouveaux réseaux de communication et de télécommunication est de mettre à disposition un contenu accessible individuellement à des moments et dans des lieux différents. Cette approche point à point et interactive remet en cause la notion de public comme étant une entité passive uniquement réceptrice de l'information. L'internaute a la possibilité de jouer réellement un rôle dans la sélection du type de contenu. Afin d'adapter cette notion de communication au public à la réalité numérique, la directive européenne sur l'harmonisation du droit d'auteur englobe dans cette notion la « *mise à disposition du public de telle manière que chaque membre du public peut y avoir accès de l'endroit et au moment qu'il choisit individuellement* ».²⁶ L'avant-projet de loi belge, qui entend modifier la loi du 30 juin 1994, reprend cette définition en modifiant l'article 1, alinéa 4 de la loi.

c. – Exceptions aux droits patrimoniaux de l'auteur (art. 22, §1^{er}, 3° et 5°)

La loi prévoit des exceptions à la faculté de l'auteur d'interdire certains usages de son œuvre. La directive du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins laisse aussi la faculté aux Etats de légiférer sur 21 exceptions parmi lesquelles celle pour copie temporaire qui est obligatoire. Parmi ces différentes exceptions de la législation belge,²⁷ nous examinerons plus particulièrement l'exception, qui autorise la communication gratuite au sein du cercle de famille, et celle qui permet, sous certaines conditions, la copie privée.

²⁵ Amendement n°46, Doc. Chambre n°473/5-91/92 (SE), pp 6-7 ; rapport DE CLERCK, pp. 192 et 195. F. BRISON ET B. MICHAUX, « De nieuwe auteurswet », *R.W.*, 1995, p. 482 ; Pour de plus ample développements, voyez F. DE VISSCHER, B. MICHAUX, *Précis du droit d'auteur et des droits voisins*, Bruxelles, Bruylant, 2000, p. 122, n°148.

²⁶ S. DUSOLLIER, « Internet et droit d'auteur », 7 mai 2001, <http://www.droit-technologie.org/>

²⁷ Certaines exceptions sortent de notre champ d'étude, et ne seront pas développées ici, tels que droit de citation (art. 21), les anthologies (art. 21, al. 3), la citation à des fins d'information (art 22 §1^{er}, 1°), l'œuvre exposée dans un lieu public (art. 22 §1^{er}, 2°) ou encore la parodie, le pastiche ou la caricature (art 22, §1^{er}, 6°)

1.- La communication gratuite dans le cercle de famille (art. 22, §1^{er}, 3°)

L'exécution privée d'une œuvre musicale n'est pas soumise à l'autorisation de l'auteur pourvu qu'elle soit gratuite et limitée au cercle de famille. Cette exception vise à permettre l'écoute d'un morceau de musique sans être soumis au diktat de l'auteur. Comme nous l'avons développé plus haut, la mise à disposition de fichiers MP3 sur Internet dépasse la notion restreinte de cercle de famille et n'entre pas dans le champ de cette exception.

2.- La reproduction des œuvres sonores et audiovisuelles dans le cercle de famille (art. 22 § 1^{er}, 5°)

La loi autorise ici la reproduction d'une œuvre sonore ou audiovisuelle à deux conditions :

- si elle est faite dans le cadre de la famille
- si elle est réservée à l'usage du cercle de famille.

Selon nous, il est donc autorisé de transformer un disque que l'on possède en MP3 pour pouvoir l'écouter sur son ordinateur de manière « privée ».

L'auteur, qui n'a plus le droit d'interdire ces reproductions, conserve néanmoins un droit à rémunération sur la vente des supports vierges et appareils utilisables pour la reproduction.²⁸ Ainsi, une rémunération est prévue, dans le cas d'un transfert d'une œuvre sonore vers un disque dur, qui serait payée par les fabricants de disques durs.²⁹

La directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins prévoit également, à l'article 5.2 b, une exception « *lorsqu'il s'agit de reproductions effectuées sur tout support par une personne physique pour un usage privé à des fins non commerciales, à condition que les titulaires de droits reçoivent une compensation équitable* ». Cette exception est également reprise par l'avant-projet de loi belge.

La distinction numérique et analogique n'a pas été jugée nécessaire dans la nouvelle directive mais le principe de compensation équitable a été conservé.³⁰ La copie numérique présente, par rapport à la copie analogique, les avantages d'être de meilleure qualité, plus facile et moins coûteuse. Si le préjudice économique risque d'être plus grand pour les auteurs, les systèmes techniques, qui sont offerts dans l'environnement numérique, permettent néanmoins souvent un contrôle de la destination et de l'utilisation de ces œuvres.³¹

²⁸ Articles 55 et 56, al. 2 de la loi du 30 juin 1994 relative aux droits d'auteur et aux droits voisins et arrêté royal du 28 mars 1996, *M.B.*, 6 avril 1996, p.8219. La rémunération à payer pour l'enregistrement sur les supports numériques est de 5 francs l'heure.

²⁹ Cette rémunération n'a pas encore d'effet utile. Voy. J. FOLON et R. BAILLY, « La musique on line : une nouvelle gestion du droit d'auteur et des droits voisins ? », *Revue Ubiquité*, mai 1999, n°2, F.U.N.D.P., p. 73.

³⁰ La distinction est cependant mentionnée dans le considérant 39 de la directive.

³¹ S. DUSOLIER, « Internet et droit d'auteur », 7 mai 2001, <http://www.droit-technologie.org/>

3. LA COMPATIBILITÉ DE LA RECHERCHE D'INFRACTIONS AU DROIT D'AUTEUR COMMISES SUR INTERNET AU REGARD DES DISPOSITIONS JURIDIQUES PROTÉGÉANT LA VIE PRIVÉE ET LES TÉLÉCOMMUNICATIONS

Les faits que nous avons relatés dans l'introduction ne manquent pas de susciter des interrogations quant au respect des dispositions législatives relatives à la protection de la vie privée et des télécommunications. Les particuliers « tracés » envisageaient de porter plainte et les parlementaires eux-mêmes se sont posé des questions sur la légitimité de telles procédures. C'est sans doute la raison pour laquelle la Commission de la protection de la vie privée, faisant usage de l'article 29 de la loi du 8 décembre 1992 relative à la protection de la vie privée, s'est saisie d'office et a rendu un avis d'initiative condamnant de telles pratiques³². Dans cette partie nous examinerons donc la compatibilité du comportement de l'IFPI avec les prescriptions des différentes législations. On gardera bien à l'esprit la problématique générale qui est bien de savoir dans quelle mesure des organismes privés peuvent-ils chercher à faire respecter les droits d'auteur dont ils ont la gestion. Il s'agit d'identifier les problèmes que fait naître une telle situation et les solutions qui peuvent éventuellement être préconisées.

3.1. LA LOI SUR LA PROTECTION DE LA VIE PRIVÉE

L'IFPI avait-elle le droit de collecter les adresses IP des utilisateurs de Napster ? Pour avoir le droit, il faut respecter le droit, en l'occurrence le droit des personnes à leur vie privée. La question de savoir si la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (loi vie privée ci-après) a été respectée par les différents acteurs en présence mérite un examen attentif.

Cette question ne revêt pas la même démarche selon que l'on parle de l'IFPI ou des fournisseurs d'accès. S'agissant de l'IFPI, il s'agit avant tout de vérifier si les agissements de l'organisation auraient dû être soumis à la loi vie privée et dans l'affirmative, quelles devaient être ses obligations. C'est donc essentiellement la question de l'applicabilité de la loi au cas d'espèce. S'agissant des fournisseurs d'accès la question est moins celle de sa soumission que celle de son respect des dispositions de la loi. On sait que les fournisseurs d'accès doivent respecter la loi vie privée mais n'ont-ils pas commis une faute dans le cadre de leur collaboration avec l'IFPI ?

Avant de commencer une remarque mérite d'être faite. Les faits se sont déroulés principalement sous l'empire de l'ancienne loi. En effet la loi du 8 décembre 1992 a été amendée en 1998 mais, à défaut d'arrêtés royaux portant exécution de cette nouvelle loi, c'est la version de 1992 qui était encore en vigueur. Si la collecte des informations par l'IFPI a eu lieu alors que l'ancienne loi était encore en vigueur, on sera néanmoins attentif aussi bien à l'ancienne version qu'à la nouvelle³³, puisque l'IFPI n'exclut pas de continuer ses recherches sur Internet³⁴. La nouvelle loi est entrée en vigueur le 1er septembre 2001, soit 6 mois après la publication de l'arrêté royal du 13 février 2001 portant exécution de la loi vie privée.

a.- Objet et sujet de la protection

La première question à se poser est la suivante : avons-nous affaire à des données protégées par la loi ?

³² Avis n°44/2001 du 12 novembre 2001, *op. cit.*

³³ En l'absence de précisions, on se réfère à la nouvelle loi.

³⁴ Notamment au moyen d'un logiciel spécial, voir infra.

1.- L'adresse IP comme une donnée personnelle

Le concept de donnée à caractère personnel est défini par l'article 1, §1er comme étant «toute information concernant une personne physique identifiée ou identifiable, désignée « personne concernée » ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »³⁵. Voyons donc si on peut parler de données à caractère personnel à propos des adresses IP.

1.- Qu'est-ce que l'adresse IP ?

Le réseau Internet utilise le protocole TCP-IP³⁶ commun à tous les ordinateurs voulant communiquer entre eux. Le schéma de base d'une (trans)action sur Internet est le suivant³⁷ : l'utilisateur de l'ordinateur connecté est un client qui adresse des requêtes à un serveur qui est le site choisi. Les requêtes elles-mêmes correspondent à des actions faites par le client sur son navigateur pour passer d'un lien à l'autre (soit en cliquant sur un lien, soit en entrant directement une adresse). Une fois la requête adressée, le serveur répond en envoyant le résultat (correspondant à la requête formulée ou à un message d'erreur si la page n'est pas trouvée). Or, pour qu'un serveur puisse envoyer le résultat à l'ordinateur qui a adressé la requête et lui seul, il doit disposer de l'adresse de cet ordinateur, c'est l'adresse IP. Le protocole TCP/IP indique que les adresses des ordinateurs connectés au réseau doivent avoir une adresse IP unique pendant une session. Cette adresse qui identifie l'internaute est donc comparable à un numéro de téléphone à la « nuance près que l'identification d'appel n'est pas désactivable³⁸ ».

On distingue deux types d'adresse IP en fonction du type d'accès à Internet. Ainsi la plupart des particuliers louent un accès à Internet, ce qui signifie que l'utilisateur, pour chaque connexion, se voit attribuer par le fournisseur d'accès un numéro IP unique qui ne changera pas pendant toute la durée de cette connexion. Par après ce même numéro pourra être attribué à d'autres internautes mais uniquement lors de sessions différentes. On parle d'adresse IP dynamique. Certains internautes (entreprises, universités, ...) par contre disposent d'une connexion permanente, par le biais d'une ligne louée par exemple. L'adresse est généralement définitive, on parle donc d'adresse IP fixe.

2.- L'utilisation de l'adresse IP par les fournisseurs d'accès

Les fournisseurs d'accès à Internet offrent aux particuliers des connexions via leur réseau de télécommunication (pstn, rnis, adsl). Les milliers de clients particuliers se voient attribuer des adresses IP dynamiques à chaque connexion. Chaque adresse ainsi que le nom de la

³⁵ Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel, telle que modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 février 1999, p.3049.

³⁶ « Transmission Control Protocol / Internet Protocol »

³⁷ L BERNAT, « vos traces sur Internet : découvrez comment vous êtes pistés sur Internet », *C.N.I.L.*, version 1.0-1998, p.24, <http://www.cnil.fr>.

³⁸ J-M DINANT, « Les traitements invisibles sur Internet », juillet 1997, p.14, <http://www.droit.fundp.ac.be/crid/eclip/Luxembourg.html>

personne à qui elle est allouée à un moment donné sont stockés dans des bases de données à partir desquelles il est aisé de retrouver soit une personne en fonction de l'adresse IP utilisée, soit à partir du nom d'un client les adresses IP utilisées, le nombre d'heures de connexion, leur répartition, . . .

3.- Adresse IP en tant que donnée à caractère personnel (“personne identifiable indirectement”)

Il n'est pas à douter que de tels fichiers soient d'une utilité primordiale pour les sociétés, principalement comme outil de gestion des services et produits offerts (marketing, étude de marché, ...). Les fournisseurs d'accès posent néanmoins un problème général au niveau des adresses IP qu'ils allouent aux utilisateurs. Une adresse IP étant un identifiant unique au moment des traitements sur Internet, les fournisseurs d'accès peuvent constituer sur cette base des fichiers contenant des informations qui ont incontestablement le caractère de données personnelles. Ces informations concerneraient *une personne physique identifiable*, c'est-à-dire, conformément au prescrit de la loi qui *peut être identifiée, directement ou indirectement*. Or la simple connaissance d'une adresse IP ne permet pas d'établir à qui elle se rapporte pour un moment donné. Par contre l'utilisation couplée de l'adresse IP et de la base de données des fournisseurs d'accès permet sans difficulté une identification précise de l'utilisateur, ou plutôt faudrait-il dire du client de l'abonnement. Il est en effet important de préciser que l'adresse IP permet d'établir que l'ordinateur connecté est celui du client qui a souscrit l'abonnement et il n'est pas impossible que ce soit une autre personne que lui-même qui l'utilise.

4.- Comment obtenir l'adresse IP ?

Nous avons expliqué auparavant comment fonctionne le logiciel Napster. Il faut encore ajouter qu'il est très facile d'obtenir l'adresse IP des personnes connectées au logiciel à un moment donné. En effet, si une fonction du logiciel permet d'obtenir certaines caractéristiques techniques d'un connecté, elle ne permet cependant pas d'accéder à son adresse IP. Il existe différents moyens d'obtenir cette information. Un simple logiciel d'analyse de trafic permet par exemple de surmonter cette difficulté. Encore plus simple, une commande Dos³⁹ (netstat) permet d'obtenir de nombreuses informations sur le trafic du réseau. Ainsi n'importe qui avec un simple PC et sans logiciel particulier peut obtenir l'adresse IP des autres utilisateurs avec qui il est en communication. Il suffit de télécharger un fichier musical et à ce moment de contrôler dans la commande Dos la provenance du fichier et donc l'adresse IP de l'ordinateur qui «offre» le fichier. Quiconque peut dès lors établir une liste des adresses IP sans cependant savoir à qui elle se rapporte dans le monde dit réel. Inutile de rappeler qu'il faut également télécharger le logiciel Napster pour arriver à ses fins.

L'IFPI Belgium aurait procédé à une recherche manuelle, telle que décrite ci-dessus, pendant une période de neuf mois. On sait que l'IFPI disposerait à présent d'un logiciel capable de pister les napstériens. Le fonctionnement du software est assez simple, il se fait passer pour un client dans les «file-sharing networks» (réseaux de partage de fichiers tel Napster) où les internautes s'échangent de la musique généralement protégée par le droit d'auteur. Il collecte alors les informations émanant des autres ordinateurs et les ajoute à sa base de données. Ce logiciel peut également surveiller les chatrooms IRC et les newsgroups,

³⁹ Dos (Disk Operating System) est un système d'exploitation créé au début des années 80 et utilisé avant l'arrivée de windows, linux, ... Les ordinateurs actuels sont encore généralement équipés de ce système.

interroger les moteurs de recherche et contrôler les sites ftp⁴⁰ à la recherche des contenus protégés. Les informations recueillies sont suffisamment précises pour permettre d'identifier les ordinateurs et déterminer qui en sont les utilisateurs avec l'aide des ISP⁴¹ (qui sont également identifiés par le programme). La base de données ainsi constituée permet des requêtes qui produisent des listes des machines contrevenantes, des adresses IP, des heures de connections, des titres des morceaux, ... et le tout classé en fonction de divers critères, les ISP ou une date par exemple. Ainsi, il est possible de demander au programme de fournir les adresses IP des machines ayant téléchargé la chanson de Jacques Brel «Amsterdam» entre le 5 mars et le 5 avril et qui ont pour fournisseur d'accès telle société. Cet exemple est certes imaginé, il n'en est pas moins réaliste, dans la mesure où l'IFPI Belgium ne s'occupe en priorité que du répertoire des artistes belges téléchargé par des internautes belges. Ce programme peut en outre poursuivre des ordinateurs qui sont connus comme contrevenants et accumuler les informations à leurs propos dans une perspective de poursuites judiciaires. Il s'agit sans aucun doute d'une arme redoutable mais elle nécessite l'aide des ISP sans lesquels aucune identification n'est possible.

5.- L' IFPI et les adresses IP

On a vu qu'il est techniquement aisé d'identifier une personne à partir d'une adresse IP, mais ce n'est en principe praticable que par les fournisseurs d'accès et opérateurs de réseaux. Cependant les moyens d'identification existent et c'est important au regard de l'exposé des motifs de la nouvelle loi. Ainsi, «une information relative à une personne est considérée comme donnée à caractère personnel tant que quelqu'un est en mesure, par quelque moyen qui puisse raisonnablement être mis en œuvre, de déterminer à quel individu se rapporte cette information. Sont donc également considérées comme «données à caractère personnel» les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne»⁴². Par conséquent, on peut conclure qu'une personne qui collecterait des adresses IP avec des informations y afférentes (consultation de tel site, échange de tels fichiers, ...), même si elle ne possède pas le moyen technique d'identifier les utilisateurs, se retrouve dans la position d'un «responsable de traitement» et la loi de s'appliquer pour autant que les autres conditions soient remplies. Une liste d'adresses IP ne constituerait donc pas des données anonymes non couvertes par la loi⁴³.

Certains auteurs défendent un autre point de vue.⁴⁴ Le caractère identifiable d'une donnée serait fonction d'une analyse intrinsèque de la donnée (quelle donnée ?) mais également extrinsèque (quel responsable de traitement placé dans une situation concrète ?). Le caractère personnel d'une donnée dépendrait de la situation particulière de chaque responsable du traitement. Nous ne partageons pas cette opinion qui ajoute une condition d'application non

⁴⁰ Site qui se comporte comme des serveurs utilisant le « file transmission protocol ». Avec ce protocole tout un chacun peut consacrer une partie de son disque dur en serveur et mettre, par exemple, des fichiers musicaux, des images ou des films à disposition des autres internautes. Le software Hotline en est un exemple.

⁴¹ Internet Service Provider : fournisseur d'accès à Internet

⁴² Exposé des motifs, *Doc.Parl.* ; Ch.Repr., Sess.ord. 1997-1998, n°1586/1, p.12.

⁴³ Selon certains auteurs cette interprétation irait à l'encontre de celle donnée dans le considérant n° 26 de la directive. La directive précise que pour déterminer si une personne était identifiable, il faut considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre soit par le responsable du traitement, soit par un tiers pour identifier la dite personne. Cela permettrait d'admettre comme anonymes des données pour lesquelles le responsable du traitement ne disposait pas de moyens techniques pour effectuer l'identification même si la possibilité d'identification existait in abstracto. Voir à ce sujet les deux interprétations possibles dans M-Boulanger H., De TERWANGNE C., Th. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, p.125.

⁴⁴ Voy notamment Etienne Wery, "La Commission vie privée n'aime pas les manières de l'IFPI de traquer les pirates sur l'Internet", <http://www.droit-technologie.org>, 17 Décembre 2001

prévue par loi et va à l'encontre de l'esprit de la loi tel qu'il ressort de l'exposé des motifs. Dans son avis, la Commission de la protection de la vie privée soutient également cette thèse.

En octobre 2000, l'IFPI a lancé une campagne visant à rappeler les droits de ses membres aux utilisateurs de Napster. Pour ce faire, près de 12000 courriers ont été envoyés vers des internautes qui ont utilisé le logiciel pour se procurer des fichiers MP3⁴⁵. Ces courriers contenaient des informations à propos desquelles on est en droit de se poser des questions. Outre l'énoncé des missions de l'IFPI et des menaces d'actions légales au cas où ne cesseraient pas les pratiques de mise à disposition publique de fichiers musicaux, voici ce que contenait ces lettres adressées aux particuliers par le biais de leurs fournisseurs d'accès :

- l'adresse IP de l'utilisateur de Napster dont l'obtention nécessite les démarches expliquées ci-dessus ;
- le surnom de l'utilisateur de Napster directement visible sur le logiciel ;
- le nom de l'Internet Service Provider que l'on connaît grâce à l'adresse IP ;
- la date et l'heure où le fichier musical était accessible sur l'ordinateur de l'utilisateur ;
- le nom du groupe dont le morceau était accessible également directement visible sur le site

Le service juridique de l'IFPI a donc «tracé» les utilisateurs belges (et fournisseur de contenu belge) de Napster et cela en mettant en œuvre des moyens qui vont au-delà de la simple navigation sur Internet. Ensuite, sachant comment faire le lien entre les adresses IP et les utilisateurs réels, l'IFPI a demandé aux fournisseurs d'accès d'envoyer les courriers sans que les responsables de l'IFPI ne prennent connaissance des identités et domiciles des utilisateurs de Napster. Ceux-ci espérant ainsi échapper à tous griefs en matière de respect de la vie privée. Certes, ils peuvent se défendre de ne pas connaître les utilisateurs réels, néanmoins cela n'a que peu d'importance selon l'interprétation que nous avons donnée ci-dessus. Puisqu'il existe un moyen raisonnable de les identifier ces données devraient tomber sous le champ d'application de la loi quand bien même cette possibilité technique n'existe qu'*in abstracto* dans le chef d'un tiers, à savoir le fournisseur d'accès⁴⁶. Nous pensons que le fait d'obtenir l'identité précise des internautes grâce aux bases de données automatisées des fournisseurs d'accès est de l'ordre du moyen raisonnable.

2.- Fichiers, traitements et responsable du traitement

1.- Fichiers

Si la notion de «fichier» a été modifiée dans la nouvelle loi, elle n'est pas pour le moins dépourvue de toute ambiguïté. Ainsi le §3 de l'article 1^{er} prévoit qu'un fichier est « *tout ensemble structuré de données à caractère personnel accessible selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* ». Si le but est toujours d'exclure les dossiers non automatisés, la loi est « muette concernant le niveau d'accessibilité à atteindre pour admettre la qualification de fichier »⁴⁷.

⁴⁵ A. JENNOTTE, «Les affaires du net font la une des prétoires», *Le Soir*, supplément multimédia du vendredi 31 décembre 1999.

⁴⁶ Dans ce sens voir S. LOUVEAUX, « Le commerce électronique et la vie privée », disponible sur le site du C.R.I.D. <http://www.droit.fundp.ac.be/crid.html>

⁴⁷ TH. LEONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution : la loi du 11 décembre 1998 transposant la directive 95/46 du 24 octobre 1995 », *J.T.*, 1999, p.5.

Selon l'article 3 §1^{er} qui détermine l'application de la loi, les traitements non automatisés de données personnelles doivent figurer dans des fichiers. Dès lors, si des dossiers « papiers » ne correspondent pas à la définition de fichiers (par manque de structure notamment) alors le traitement peut échapper à l'application de la loi. Mais l'article 3§1 précise également que la condition de fichier n'a pas à être respectée si le traitement est automatisé (pour tout ou en partie). Par conséquent, lorsque des données sont au minimum collectées sur un ordinateur, on a affaire à un traitement automatisé. Ainsi jouer sur ce concept de fichiers ne pourrait pas constituer une échappatoire pour l'IFPI ⁴⁸.

2.- Traitements

La notion de traitement vise *«toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel »*⁴⁹. Avec une définition qui élargit autant le champ d'application, «il est difficile d'imaginer des opérations sur les données à caractère personnel qui ne constitueraient pas un traitement au regard de la loi »⁵⁰.

La notion de traitement est tellement large qu'elle ne pose pas de véritable problème quant à savoir si les démarches de l'IFPI rentrent dans son champ⁵¹. L'IFPI a au minimum collecté, conservé et organisé les données concernées. L'ancienne notion était certes moins large, mais incluait également de telles démarches.

3.- Responsable du traitement

La loi définit les différentes personnes concernées par la loi. Le premier et principal intéressé (car destinataire de la plupart des obligations légales) est le responsable du traitement à savoir *«la personne physique ou morale , l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »*⁵². Cette notion de responsable remplace celle de maître du fichier dans l'ancienne loi.

Il semble que l'on puisse aisément considérer l'organisation comme responsable du traitement dans la mesure où les deux critères se retrouvent également dans son chef. Elle décide d'utiliser les données collectées afin d'avertir les utilisateurs de Napster et éventuellement de transmettre les données au Computer Crime Unit dans le cadre de poursuites judiciaires. Par ailleurs, l'organisation décide également par quels moyens le traitement est effectué. A ce titre IFPI Belgium agit de manière autonome, décidant elle-même des moyens à mettre en œuvre pour réaliser les objectifs qui sont les siens (connecter un ordinateur au réseau, chargement du logiciel Napster, stocker les informations sur le disque dur, ...). Par ailleurs elle dispose d'une personnalité juridique distincte, ce qui constitue un

⁴⁸ Ce ne serait pas la première fois que cette notion est matière à controverse, ainsi la seule affaire belge ayant donné lieu à un arrêt de la Cour de Cassation portait précisément sur la portée de la définition du « fichier » (voy.Cass. (1^{ère} ch.), 16 mai 1997, *J.T.*, p.779)

⁴⁹ Art.1^{er} §2 de la loi.

⁵⁰ S. LOUVEAUX, *op.cit.*, p.5.

⁵¹ La notion est-elle trop large ? voir en ce sens M-H.BOULANGER, C. DE TERWANGNE, TH. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, *op.cit.*, p.125 et 126 ; M-H.BOULANGER, C. DE TERWANGNE, « Internet et le respect de la vie privée », in *Internet face au droit*, Diegem-Namur, Story scientia-C.R.I.D., Cahier du C.R.I.D., n°12, 1007, p.198 et 199.

⁵² Article 1^{er} §4 de la loi.

élément de plus en faveur de sa qualification de responsable du traitement. Si on retrouve les deux critères dans le chef d'une seule entité, on évite ainsi les difficultés issues de situations où la décision des finalités revient à une entité (tête de l'organisation par exemple) et la décision des moyens à une autre entité (filiale nationale).

b.- Champ d'application matériel et personnel

Dernière question à passer en revue pour s'assurer que la loi doit s'appliquer au cas IFPI : les exceptions au champ d'application matériel et personnel. L'article 3§1^{er} précise que la *loi s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier*. Ce même article prévoit différentes exceptions totales ou partielles au champ d'application. Ainsi le §2 prévoit une exception pour les activités personnelles ou domestiques. La constitution de fichier en vue d'éventuelles poursuites judiciaires ne rentre évidemment pas dans le cadre des telles activités. Ce paragraphe ne concerne de toute façon que les personnes physiques. L'exception partielle pour des fins de journalisme ou d'expression artistique ou littéraire ne trouve pas non plus à s'appliquer. Les trois autres exceptions concernent les services de renseignements, les services de police et le centre européen pour enfants disparus et sexuellement exploités (§4, §5 et §6). Dans le cas qui nous intéresse, le parquet intervient mais pas à titre de responsable du traitement, tout au plus peut-on le considérer comme destinataire. Aucune exception ne s'appliquera pour faire échapper l'IFPI aux obligations qui sont les siennes en vertu de la loi.

Un autre point mérite d'être soulevé. En effet, un régime particulier est prévu pour les données dites sensibles c'est-à-dire les données sensibles au sens strict, les données judiciaires et les données médicales⁵³. Or, les données récoltées sur Internet sont des données relatives à des suspicions ayant trait à des infractions. Elles constituent à ce titre des données judiciaires, dont le traitement est interdit, sous réserve d'exceptions strictement réglementées par la loi. L'avis de la commission examine en profondeur les conséquences de cette qualification des données. Sous l'empire de la loi non modifiée une personne physique ou morale pouvait traiter des données judiciaires, aux seules fins de gestion de son propre contentieux, lorsque ce traitement avait pour objet « *les litiges soumis aux Cours et tribunaux ainsi qu'aux juridictions administratives* »⁵⁴. En ce qui concerne la condition qui est de se trouver dans le cadre d'un litige soumis aux cours et tribunaux, cette condition ne semble pas remplie dans la mesure où l'on se trouve au stade de l'identification des internautes afin de faire parvenir les avertissements. Autre condition à respecter, l'IFPI agit-elle dans le cadre de son propre contentieux ? Cette condition est déterminante puisque l'article 8 nouveau, ne mentionne plus la première condition relative à l'existence d'un litige soumis aux cours et tribunaux. Sur base de l'exposé des motifs, la commission estime que le législateur n'a pas voulu que l'on interprète le nouveau libellé dans un sens plus large que celui de l'« ancien » article 8 et que le contentieux doit, à tout le moins, se situer dans une phase préparatoire à un litige devant une cour ou un tribunal. Elle en conclut que si ces conditions permettent à une maison de disques, à l'IFPI ou à la SABAM de traiter des données relatives à une infraction précise qu'elles ont pu constater, dans la mesure où elles se situent dans une phase au moins préparatoire à un litige, elles ne permettent pas de rechercher systématiquement et de façon proactive des

⁵³ On renvoie aux études de Th. LEONARD, Y. POULLET, « La protection des données ...*op.cit.* et de M-H.BOULANGER, C. DE TERWANGNE, Th. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, p.125.

⁵⁴ article 8, §1^{er} 1° et §3

données à caractère personnel sur Internet dans le but de déceler des infractions au droit d'auteur⁵⁵.

c.- Les principes de légitimité et de conformité

Rappelons brièvement les principes qui gouvernent la protection accordée par la loi.⁵⁶ Le principe de finalité est le principe fondamental de la loi. On y distingue deux composantes : le principe de légitimité et celui de conformité. S'agissant du premier principe l'article 4 §1^{er} 2° prévoit que *les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités*. Il est complété par l'article 5 qui prévoit que les traitements ne peuvent être poursuivis que dans l'un des cas visés par cette disposition. Il faut signaler que «le fait de remplir l'une des conditions de l'article 5 n'implique pas que l'exigence de légitimité de l'article 4, 2° soit d'office rencontrée. Les différentes dispositions s'appliquent en effet de manière cumulative»⁵⁷.

Le deuxième principe est celui de conformité. La conformité c'est un lien suffisant entre les données et la finalité poursuivie. C'est pourquoi l'article 4 §1,3° dispose que les données à caractère personnel doivent être *«adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement»*. Le reste de l'article précise la «qualité» que les données doivent présenter (exactitude et mise à jour, durée de conservation).

A travers ces deux principes la loi impose une transparence des traitements qui interdit que «la personne ne soit laissée dans la méconnaissance de l'utilisation des données la concernant»⁵⁸. De telles exigences mettent l'IFPI dans une situation quelque peu inextricable. Ainsi l'IFPI constitue des fichiers sur les utilisateurs de Napster à leur insu alors que pour respecter la loi vie privée il faudrait les avertir. Mais pour les avertir, il faut les identifier et cela nécessite le concours des fournisseurs d'accès. Ces derniers doivent donc donner les identités correspondantes aux adresses IP et cela en violation de la loi vie privée, de leurs conditions générales de vente et d'autres dispositions législatives.

d.- La recherche systématique et proactive de données à caractère personnel est interdite

Si on accepte la qualification attribuée aux données par la Commission, force est de constater qu'un tel traitement est interdit dans la mesure où aucun litige n'est engagé, pas même à titre préparatoire. On peut discuter cette qualification, mais même en admettant que ce traitement soit autorisé, la situation de l'IFPI reste malaisée et cela pour trois raisons. Premièrement, la nature des données collectées. On a démontré que les adresses IP doivent être considérées comme des données personnelles soumises à la protection de la loi. Ce type de donnée n'est pas une donnée anonyme, exclue de la loi, elle s'apparente plus à une donnée codée. Mais se pose alors la question de savoir comment respecter le prescrit de la loi sans connaître l'identité des personnes concernées. On ne peut que s'étonner de ce paradoxe de la

⁵⁵ Avis n°44/2001, *op.cit.*, pp. 3 et 4.

⁵⁶ Voy. TH. LEONARD, Y. POULLET, «Les libertés comme fondements de la protection des données nominatives», in F. RIGAUX, *La vie privée une liberté parmi les autres ?*, Travaux de la faculté de droit de Namur, n°17, Bruxelles, Larcier, 1992, p.231 et s.

⁵⁷ S. LOUVEAUX, «Le commerce électronique et ...», *op.cit.*, p.9 et voy. «A business guide to changes in european data protection legislation», CRID-CULLEN INTERNATIONAL, Kluwer Law International, 1999, p.46.

⁵⁸ TH. LEONARD, Y. POULLET, «La protection des données ...*op.cit.*, p.20.

loi qui impose aux traitements de données sans «identité» des obligations qui nécessitent l'identification des personnes concernées. La deuxième difficulté rencontrée par l'IFPI réside dans la manière de mener son action. L'intérêt étant de surprendre les internautes «coupables de piraterie», on voit mal comment atteindre ce but en prévenant au préalable ceux-ci qu'ils vont faire l'objet d'un traçage. Enfin troisième difficulté : comment obtenir l'aide des fournisseurs d'accès sans que ceux-ci ne soient contraints de passer outre les obligations de la loi vie privée, reprises en partie dans leurs conditions générales de vente. Cette difficulté est liée à la première puisque le respect des obligations nécessite l'identification des internautes et que cette identification passe nécessairement par les fournisseurs d'accès.

e.- L'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, avait été modifiée par la loi du 11 décembre 1998 dans le but de transposer la directive générale 95/46/CE du 24 octobre 1995. Mais cette nouvelle mouture de la loi n'était pas d'application faute d'arrêté portant exécution de celle-ci. C'est désormais chose faite avec la publication au moniteur belge de ce 13 mars 2001 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. On souligne certains éléments en relation avec ce que nous avons évoqués⁵⁹.

1. L'arrêté royal introduit la notion de données codées ou non codées. Les «données à caractère personnel codées» sont celles qui ne peuvent être mises en relation avec une personne identifiée ou identifiable que par l'intermédiaire d'un code ; les autres sont non codées (article 1^{er}, 3^o) ;
2. L'arrêté royal introduit la notion de données anonymes, c'est-à-dire les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel (article 1^{er}, 4^o) ;
3. Le droit d'accès est modernisé puisqu'il peut se faire dorénavant par tout moyen de télécommunication : «Toute personne justifiant de son identité a le droit d'obtenir, dans les conditions prévues par la loi, communication de l'information visée à l'article 10 de la loi en adressant une demande signée et datée qu'elle remet sur place, ou qu'elle envoie par tout moyen de télécommunication (...)»(article 32) ;
4. La déclaration à la Commission est modernisée puisque la procédure et les coûts sont différenciés selon que la remise a lieu sur support papier ou sur support magnétique ;

L'arrêté royal est entré en vigueur le premier septembre 2001.

⁵⁹ Ce passage reprend les informations contenues dans E. WERY, « La nouvelle loi «vie privée» va entrer en vigueur : l'arrêté d'exécution est publié», *Droit et nouvelles technologies*, 14 mars 2001, www.droit-technologie.org

3.2. LES AUTRES LEGISLATIONS

Un organisme privé est-il en droit de suivre les utilisateurs de Napster et d'enregistrer les données ainsi récoltées ? Les particuliers «tracés» ne sont pas les seuls à se poser cette question, certains parlementaires de la Chambre ont en effet interpellé le ministre de la justice en ce sens : *«pouvons-nous accepter que les entreprises privées assument un rôle de policier et qu'elles fassent poursuivre les gens ? N'y a-t-il pas infraction à la législation sur le respect de la vie privée ? Quel suivi donnera-t-on à ses démarches ? Donnera-t-on la priorité aux poursuites»* ou encore *«êtes- vous au courant d'accords conclus entre le parquet et des groupes d'intérêt en vue d'intervenir à l'encontre de ces pratiques ?»*⁶⁰. Selon le ministre Verwilghen *«les adresses IP étant attribuées à un appareil et non à une personne, cette matière ne ressort pas strictement à la loi sur la vie privée»*. Nous nous permettons de ne pas partager cet avis puisque nous pensons, au contraire, que les adresses IP sont assimilables à des données personnelles. En outre, on peut s'interroger sur la légalité des poursuites qui seraient intentées sur la base de constatations réalisées en infraction à la loi sur la vie privée. En effet, la recherche et le constat des infractions doit se faire dans le respect de la loi sous peine d'entacher de nullité les poursuites ainsi entamées.

De plus, la légitimité de l'action menée par l'IFPI se pose également au regard d'autres dispositions protectrices de la vie privée et plus particulièrement des télécommunications. Ces dispositions mériteraient à elles seules un examen approfondi, tel n'est pas l'objet de cette contribution.

a.- L'article 314 bis du Code pénal

L'article 314 bis du Code pénal punit *« d'un emprisonnement de six mois à un an et d'une amende de deux cents francs à dix mille francs ou d'une de ces peines seulement, quiconque (...) intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications »*.

Le champ d'application matériel de cette disposition est large et vise les transmissions de données sur Internet⁶¹. L'exposé des motifs⁶², comme les commentateurs de cette loi admettent que les communications ou télécommunications visent également *«la transmission électronique de données dans des ordinateurs ou des réseaux d'ordinateurs»*⁶³.

Dans l'exposé des motifs de cette loi, *«les communications ou télécommunications sont privées lorsqu'elles ne sont pas destinées à être entendues par tout un chacun»*⁶⁴. Peu importe dès lors également que le mode de transmission se fasse par un réseau de télécommunication

⁶⁰ Questions / réponses de la Chambre (3^{ème} session de la 50^{ème} législature/ CRABV 50 PLEN 109), 15/02/2001, disponible sur le site de la Chambre www.lachambre.be

⁶¹ T. LEONARD, «E-marketing et protection des données à caractère personnel», *Droit et nouvelles technologie*, 23/05/2000, www.droit-technologie.org, p.23.

⁶² *Doc.Parl.*, Sénat, sess.ord.1992-1993, n°843-1, p.7.

⁶³ Voy. Par exemple, H-D. BOSLY, D.VANDERMEERSCH, La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées », *R.D.P.*, 1995, p.304, note 11 ; T. HENRION, «les écoutes téléphoniques», *J.T.*, 1995, p.209, note 26 et 28 ; R. FELTKAMP, M. FLAMEE, «Telecommunicatie, privacy en bescherming van persoonsgegevens – Deel I. Bescherming van het communicatiegeheim », *A.&M.*, 1999, p.173 ; P. LAMBERT , «Bescherming van prive-(tele)communicatie », in *Recente ontwikkelingen in informatica-en telecommunicatierecht*, Icri, Brugge, Die Keure, 1999, p.&85 et 193 cités dans TH. LEONARD, «E-marketing et protection...», *op.cit.*, p.23.

⁶⁴ *Doc.Parl.*, Sénat, sess.ord.1992-1993, n°843-1, p.7.

privé ou public. Les critères à prendre en considération sont le contexte et les intentions des parties⁶⁵. Le caractère public du réseau des utilisateurs de Napster ne s'oppose pas à l'application de cet article. Le problème se situe ailleurs. L'IFPI dans son travail de traçage n'intervient pas comme un tiers qui surveillerait les échanges entre les napstériens, il se fait lui-même passer pour un utilisateur. Il prend donc part directement à la télécommunication privée. Le napstérien offrant les fichiers ignore que le client n'est autre que l'IFPI qui enregistre les données relatives à ce téléchargement. L'article 314bis peut poser problème dans ce cas d'espèce tant les conditions ne semblent pas réunies pour pouvoir s'appliquer.

b.- L'article 109 ter D de la loi du 21 mars 1990 portant réforme de certaines entreprises publiques économiques.

L'article 109 ter D de la loi du 21 mars 1990 portant réforme de certaines entreprises publiques économiques énonce que : *« sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit à quiconque, qu'il agisse personnellement ou par l'entremise d'un tiers : 1° de prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunications, en provenance d'autres personnes et destinées à celle-ci ; 2° de transformer ou de supprimer frauduleusement par n'importe quel procédé technique l'information visée au 1° ou d'identifier les autres personnes ; 3° de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne ; 4° de révéler ou de faire un usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non visées aux 1°, 2° et 3°, de les modifier ou de les annuler »*. Les données en matière de télécommunications visées au point 3 sont des données de trafic, comme le lieu de la transmission, un numéro secret, ... à l'exclusion des données généralement connues comme le nom, l'adresse, ... Des données telles que celles qui nous intéressent (numéro TCP/IP), tombent dès lors sous le champ d'application de cette disposition⁶⁶. Cette disposition a un champ d'application plus large et pourrait donc s'avérer plus utile que celle du code pénal. Comme le relève la Commission, « le fait que la personne responsable de la prise de connaissance soit ou non partie à la communication est sans relevance dans le cadre de cette disposition ». En effet le point 4 *interdit à quiconque de faire un usage quelconque (...) des données (...) visées aux 1°, 2° et 3° (...) sous réserve l'autorisation de toutes les personnes directement ou indirectement concernées par l'information*. Le consentement de l'internaute s'impose comme une condition pour ne pas violer cette disposition. Les démarches de l'IFPI apparaissent donc en contradiction avec cette disposition.

Seuls les agents ayant la compétence d'officier de police judiciaire peuvent procéder à une interception de données de télécommunication protégées par la loi. Il faut, dans ce cas, que l'on soit en présence d'une infraction pénale telle que prévue à l'article 80 de la loi sur le droit d'auteur. Cette hypothèse demeure aléatoire car il faut que soit démontrée la matérialité des faits et l'intention frauduleuse ou malveillante de l'auteur. Il est possible que le juge ne reconnaisse pas le caractère pénal de l'infraction constatée par le parquet. Par conséquent, des moyens judiciaires particulièrement contraignants pour la liberté des citoyens et, en principe réservés à la recherche des infractions pénales, auraient été mis à profit pour mettre à jour des infractions ressortant du domaine civil.

⁶⁵ TH. LEONARD, «E-marketing et protection...», *op.cit.*, p.24.

⁶⁶ TH. LEONARD, «E-marketing et protection...», *op.cit.*, p.26.

c.- L'article 109 ter E de la loi du 21 mars 1990 portant réforme de certaines entreprises publiques économiques et le projet de loi portant application de cet article.

L'article 109 ter E de la loi du 21 mars 1990 portant réforme de certaines entreprises publiques économiques prévoit que les actes visés tant à l'article 314 bis du Code pénal qu'à l'article 109 ter D de la loi du 21 mars 1991 ne sont pas punissables si la loi le permet ou lorsque les données sont utilisées pour contrôler le bon fonctionnement du réseau ou assurer la bonne exécution du service de télécommunication.

Le projet d'arrêté royal portant application de cet article, dans le cadre des demandes et réquisitions judiciaires résultant des articles 46bis, 88bis, 90ter et suivants du Code d'instruction criminelle, oblige chaque opérateur de réseaux de télécommunications (par exemple un fournisseur d'accès à Internet) d'être en mesure techniquement de repérer, de localiser, d'écouter, de prendre connaissance et d'enregistrer des télécommunications privées. Ce même projet prévoit la mise en place d'un accès direct et automatisé des autorités judiciaires aux banques de données des opérateurs et fournisseurs de service. L'adoption de cet arrêté, en obligeant les fournisseurs d'accès à identifier les clients et à conserver une trace des communications, ne fera que confirmer ce que nous avançons : le numéro TCP/IP est bien une donnée à caractère personnel⁶⁷.

d.- L'article 105 nonies de la loi du 21 mars 1990 portant réforme de certaines entreprises publiques économiques et le projet de loi portant application de cet article.

« §4 : ...les données visées peuvent être traitées par l'opérateur d'un réseau public de télécommunication ou par le fournisseur d'un service de télécommunication offert au public pour détecter les fraudes.

Les données traitées pour détecter les fraudes sont communiquées aux autorités compétentes pour la recherche ou la poursuite d'infractions pénales au cas où il y a indication qu'une infraction pénale a été ou pourrait être commise. »

Cet article permet la constatation par les fournisseurs d'accès de certains actes présumés illégaux et leur communication aux autorités compétentes, c'est-à-dire les autorités judiciaires. Par contre, il ne leur donne pas des pouvoirs d'investigation propres qui leur permettraient d'effectuer des recherches d'initiative et leur interdit également de transmettre de telles données à une organisation qui ne relève pas du pouvoir judiciaire.

e.- La directive 2000/31/CE du 8 juin 2000 relative au commerce électronique.

Cette directive prévoit à charge des fournisseurs de service de télécommunication une obligation d'agir promptement dans le cas d'une constatation d'une violation de la loi. Elle n'autorise nullement les fournisseurs d'accès à suppléer aux services de police dans la recherche des infractions, notamment dans le cadre d'une collaboration avec une organisation qui ne relève pas du pouvoir judiciaire⁶⁸.

⁶⁷ S. LOUVEAUX, « Le commerce électronique..., *op.cit.*, p.4.

⁶⁸ Article 13 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *Journal officiel* n°L 178 du 17/07/2000, p.0001-0016.

CONCLUSION

Napster a ravivé le rêve d'un Internet pensé comme un nouveau monde virtuel libéré des contraintes et des règles du passé. Dans ce cyberspace idéal, tout pourrait s'échanger et se partager, et toute la communauté reliée en réseau aurait un accès gratuit à la musique et à la culture en général. Les partisans de cette joyeuse anarchie ont dû vite déchanter : l'adoption de multiples législations et différentes décisions judiciaires, dans ce domaine, sont venues rappeler qu'Internet n'est pas une zone de « non-droit ».

Napster n'a pas échappé à ce mouvement de rééquilibrage entre cette utopie de gratuité et de libre d'accès et, d'autre part, le respect du droit et des règles existantes. Ainsi, le droit d'auteur était sans conteste violé par ce logiciel d'échange de fichiers, la diffusion et la reproduction de la musique par Internet, sans autorisation des auteurs, restent illicites. Il n'est pas question ici de contester les prérogatives légitimes des auteurs, mais de prendre conscience de l'ensemble des droits qui entrent en jeu dans le monde des réseaux.

Il faut garder à l'esprit que les moyens mis en œuvre pour protéger le droit d'auteur peuvent présenter des atteintes à d'autres droits fondamentaux, tel que le respect de la vie privée. En effet, Napster est basé sur une nouvelle technologie qui réalise des échanges directement entre particuliers. Le développement de ce type de relations horizontales, relativement récent dans le paysage de l'Internet, risque d'accroître les questions de respect de la vie privée. Cette problématique se posera de manière d'autant plus accrue lorsque l'offre de contenu numérique protégé par le droit d'auteur disponible illégalement. Ainsi, on peut imaginer que des organismes privés, défendant les intérêts des producteurs de film, des créateurs de logiciels ou de jeux, cherchent aussi à détecter les infractions qui sont faites à leurs droits. Si cette recherche d'infractions s'avère de plus en plus nécessaire, il est souhaitable qu'elle se déroule dans un cadre légal. Dans cet optique, il nous paraît plus approprié, qu'elle soit réalisée par une société de gestion, telle que la SABAM, dont les statuts et les missions sont régis par la loi. En outre, ces sociétés disposent d'agents agréés par le ministre et assermentés. Des aménagements législatifs seraient nécessaires pour permettre aux sociétés de droit d'auteur de constater ces infractions propres à l'environnement numérique. En effet, comme le conclut la Commission de la protection de la vie privée dans son avis, « dans l'état actuel du droit, il appartient aux autorités judiciaires d'effectuer toutes investigations à caractère général qui pourraient mener à constituer une liste de personnes responsables d'infractions au droit d'auteur ».

Les différents angles d'approche de cette affaire, que ce soit sous le prisme des droit d'auteur ou du droit au respect de la vie privée, conduisent à nous poser des questions sur les rapports qu'entretiennent les libertés publiques et les nouvelles technologies. Internet et son contexte favorisent l'émergence de nouveaux dangers en matière de vie privée. Non seulement les risques anciens sont accrus mais de nouveaux risques apparaissent également. Les nouveaux acteurs et les nouvelles possibilités technologiques créent des menaces inédites pour la vie privée (cookies, mouchard, ...). Mais ces possibilités technologiques sont autant

d'armes de marketing redoutables et d'outils efficaces au service de l'économie des entreprises

Une facette essentielle du droit d'auteur réside dans son côté pécuniaire et par conséquent son aspect commercial. Car c'est essentiellement de cela dont il est question ici. Une fois de plus un équilibre doit être trouvé entre les prétentions de chacun. Le débat est complexe et de taille. Deux sphères de droits et d'intérêts s'opposent et doivent s'accorder. Nous pensons que la priorité doit être donnée à la vie privée dans la mesure où cette liberté sous-tend d'autres libertés et concerne tout un chacun dans ce qu'il a d'intime et personnel. Le respect de la vie privée est une composante fondamentale de la liberté au sens démocratique du terme. Il faut donc trouver un équilibre au sein duquel le droit au respect de la vie privée fasse l'objet d'une protection toute particulière.